AFRL-RI-RS-TM-2008-5
In House Interim Technical Memorandum
February 2008

COALITION NETWORK MANAGEMENT SYSTEM

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

NOTICE AND SIGNATURE PAGE

AFRL-RI-RS-TM-2008-5 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/	/s/
FRED L. MOULTON Chief, Networking Technology Branch	WARREN H. DEBANY, JR. Technical Advisor, Information Grid Division Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
Feb 2008	Interim	Dec 06 – Dec 07

4. TITLE AND SUBTITLE

COALITION NETWORK MANAGEMENT SYSTEM

5a. CONTRACT NUMBER
In-House

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
62702F

6. AUTHOR(S)

Peter J. Fitzgerald

5d. PROJECT NUMBER
4519

5e. TASK NUMBER
CN

5f. WORK UNIT NUMBER
MS

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
AFRL/RIGC
525 Brooks Rd
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/RIGC
525 Brooks Rd
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TM-2008-5

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# WPAFB 08-0345

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Under the auspices of The Technical Cooperation Program, a Project Arrangement (PA), entitled Coalition Command Control and Communications Demonstration Environment (CC3DE), between the US, Australia and Canada was created and realized from 2000 to 2003. These three nations collaborated on a Coalition Network Management System (CNMS) under the CC3DE PA. A new PA, entitled Policy Enabled Coalition Communications (PECC), will incorporate the United Kingdom and will iterate the design and concept of CNMS. As of this interim report, the PA still has not been signed due to export control language differences between nations. It is expected the PA will be signed in early 2008. Despite the limitation of an unsigned PA, AFRL has moved forward with in-house work on policy-based solutions for the coalition environment, to include: designing a modern service oriented architecture (SOA) for the coalition enterprise; identifying requirements for secure, cross-domain exchange of SOA protocols; begin design of reasoning resource monitors using semantic technology; and creating a NM protocol generator to test NM tool scalability.

15. SUBJECT TERMS
Coalition network management, network management, policy-based networking

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Peter J. Fitzgerald
U	U	U	UL	14	19b. TELEPHONE NUMBER (*Include area code*) N/A

TABLE OF CONTENTS

FIGURES AND TABLES

ABSTRACT

Under the auspices of the Technical Cooperation Program, Command, Control, Communications and Information Systems Group, Technical Panel 8, a Project Arrangement (PA) titled Coalition Command Control and Communications Demonstration Environment (CC3DE) between the US, Australia and Canada was created and realized from 2000 to 2003. Those three nations collaborated on a Coalition Network Management System (CNMS) under the CC3DE PA. A new PA, entitled Policy Enabled Coalition Communications (PECC), will incorporate the United Kingdom and will iterate the design and concept of CNMS. As of the writing of this interim report, the PA still had not been signed due to export control language differences between nations. It is expected the PA will be signed by early 2008.

This report describes in-house work performed by Air Force Research Lab (AFRL) to explore policy-based network management (NM) solutions within the coalition environment. Despite the limitation of an unsigned PA, AFRL has moved forward with several developments, to include: designing a more modern service oriented architecture (SOA) for policy-enabling the coalition enterprise environment; developing requirements for secure cross-domain exchange of SOA protocols to fit this new model; leveraging advances in semantic technology to begin design of reasoning NM resource monitors; and finally creating an NM protocol generator (using Internet Protocol version 6) to test the scalability of NM tools.

SUMMARY

Under the auspices of the Technical Cooperation Program, Command, Control, Communications and Information Systems Group, Technical Panel 8, a Project Arrangement (PA) titled Coalition Command Control and Communications Demonstration Environment (CC3DE) between the US, Australia and Canada was created and realized from 2000 to 2003. Those three nations collaborated on a Coalition Network Management System (CNMS) under the CC3DE PA. A new PA, entitled Policy Enabled Coalition Communications (PECC), will incorporate the United Kingdom and will iterate the design and concept of CNMS. As of the writing of this interim report, the PA still had not been signed due to export control language differences between nations. It is expected the PA will be signed by early 2008.

This report describes in-house work performed by Air Force Research Lab (AFRL) to explore policy-based network management (NM) solutions within the coalition environment. Despite the limitation of an unsigned PA, AFRL has moved forward with several developments, to include: designing a more modern service oriented architecture (SOA) for policy-enabling the coalition enterprise environment; developing requirements for secure cross-domain exchange of SOA protocols to fit this new model; and the use of the next generation internet protocol, IPv6 within the work.

INTRODUCTION

The PECC effort will progress the state of the art in network resource management, especially for coalition operations. This effort will align national research and development agendas, and improve interoperability in multi-national coalition operations. The main objectives are:

1. Demonstrate how network and traffic management can be partially automated to reduce the number of people required whilst also improving responsiveness, effectiveness and resilience, especially in a mixed high and low bandwidth environment over multiple bearer types.
2. Demonstrate how coalition network and traffic management can be achieved within a security architecture that is representative of US-led coalition operations.
3. Demonstrate how a coalition commander can be given visibility and control of the coalition network, with an interface that is appropriate for a military officer with military concerns rather than a technical expert.

The main technical thrust is to investigate a scalable, distributed network management and control approach that would address policy-enabled networking, integration of dissimilar bearer services, and management & security across different coalition domains. The results of this investigation will provide input to the formulation of future coalition network architectures.

METHODS, ASSUMPTIONS, AND PROCEDURES

The PECC project will operate and demonstrate at the enterprise level, endeavoring to achieve network management across the coalition infrastructure, giving a coalition commander full visibility and control over their network.

Specific scopes as related to main objectives:

1. Policy-enabled Network Control: Integrate policy-enabled coalition network management environment; continue development of more robust policy resolution methods; increase policy granularity to be more tailored to individual threats
2. Integrating Dissimilar Bearer Services: Integrate dissimilar bearer services; develop/expand military quality of service (QoS) routing and cost functions; develop/expand bandwidth management functions
3. Management and Security across different security domains: Develop/expand capability to dynamically manage the security between different domains; research potential for dynamically created groups while maintaining security boundaries

Task Distribution

Contributions of concepts, capabilities, and/or components are below.

1. Australia will:
    a. Research results, experiments and/or demonstrations of key issues affecting different routing strategies as applied to deployed tactical networks incorporating bearer services of differing characteristics.
    b. Develop an extension of the Military Bandwidth Broker (M-BB) functionality to provide (as much as possible) seamless QoS to mission-critical services whose traffic flows need to be switched between bearers of different characteristics in a dynamic fashion.
    c. Develop and demonstrate, as a contribution to the joint effort, a capability allowing the top level communications command hierarchy to monitor the status of network resources and use a policy to dynamically reallocate the resources at a coarse level and in accordance with mission priorities.
2. Canada will:
    a. Investigate a capability that each bearer service component needs to allow QoS over that bearer service.
    b. Design components that optimize network and transport protocols to improve traffic performance over the various bearers being used.
    c. Develop a component that enables management and policy-control of QoS across an integrated infrastructure consisting of a variety of bearer services.
    d. Create a demonstrator application that manages all aspects of the QoS components.

3. UK will:
    a. Configure an (existing) UK test-bed to represent UK networks. This test-bed will also have IPv6 capabilities to emulate possible future transition of UK systems to IPv6. This test-bed is provided with means to interconnect with other-nations' test-beds via ISDN and Internet.
    b. Develop a Coalition Information Infrastructure Management System (CIIMS) to manage the above UK emulated networks and interact with other nations' management systems, both as a subordinate to a foreign coalition manager and as the coalition manager.
    c. Design a component of the CIIMS that manages and policy-controls QoS across several bearer services in national and coalition scenarios—and integrate this with the US C2RMS.
    d. Enhance the UK test-bed to provide a Computer Network Defense capability for the UK networks represented thereon.
    e. Integrate computer network defense management with Network Management in the UK CIIMS, and use it to support joint research on network defense through the use of policy-based techniques.
4. US will:
    a. Make use of an improved and enhanced guard, capable of securely operating on both sides of the nation/coalition domain boundary
    b. Design a service-oriented architecture framework in which to install each nation's components with a C2RMS integration module to manage policy control components.
    c. Design a component for deploying/querying policy and management information.
    d. Develop a means to dynamically form secure communities of interest within the coalition (i.e. dynamic group formation)
    e. In accordance with evolving DoD QoS standards, develop a component that manages access and QoS across heterogeneous bearers, to include constrained Line-of-Sight (LOS) and Extended LOS bearers.
    f. Develop an interface between mobile ad hoc tactical networks and fixed infrastructure.
5. Joint contributions will:
    a. If sensible and possible: update software/hardware to support a dual-stack environment that enables both Internet Protocol (IP) version 4 (IPv4) and IPv6; ensure capabilities are policy-enabled; follow best-practice methods, to include Internet Engineering Task Force (IETF) Request For Comment (RFC) standards (or equivalent).
    b. Continue development and expansion of policy-enabled networking, especially in connection with the rapid formation, optimization and defense of coalition networks. Joint demonstration of capability enhancement.
    c. Integrate dissimilar bearers within a coalition network scenario to enable performance optimization and provide resilience. Joint demonstration of capability enhancement.

d. Demonstrate capability-based scenarios that meet the demonstration needs of all the coalition partners.
e. Determine the procedures for developing, installing, using, and documenting the PECC environment software and hardware.
f. Demonstrate the concept of a high level capability, available to the top level communications command hierarchy, to assess multiple domain (national and coalition) network and information system status to assist mission planning. In addition, allows the changing of high level policies, reallocating resources at a coarse level, in accordance with mission priorities. This capability should enable interfacing with typical applications/tools resident within Network Operations Centers.
g. Enhance each nation's test-beds to include such security functionality (cryptography, firewalls, computer network defense, authentication, etc.) as would be appropriate at the interconnections between national systems in a coalition network. These functions may be emulated, or use lower-fidelity commercially or openly available substitutes for military-grade functions where necessary. In particular, for interconnection of Allies with the US, these functions need to be consistent with the Global Information Grid – Enterprise Services (GIG-ES) and GIG – Information Assurance (GIG-IA) architectures, which the US will verify.
h. Perform demonstration and/or integration of developed capabilities/components on the Combined Federated Battle Lab Network (CFBLNet) with interested nations.
i. Provide end of year-two joint analyses and report as well as joint final analyses and reports

Scheduling of Tasks

For period of activity, there will be three spirals, each 12 months in duration, and each including the following overlapping phases:

1. Analyze - Resolve objectives, discuss alternatives, and identify constraints/risks (first 4 months of spiral)
2. Evaluate - Evaluate design alternatives and their risks (months 2 - 5 of spiral)
3. Develop - Develop next evolutionary prototype (months 5 - 12 of spiral)
4. Review - Review outcome and plan next cycle (months 11 - 12 of spiral)

During spiral 1, projected to begin upon signing of PA:

- Jointly construct a fully integrated test bed by adding UK to the current US, Canada, and Australia integrated test beds. Following the joint engineering of the new system, if required, the UK will be provided any applicable disclosable information per the CC3DE PA.
- Jointly review the collaborative policy-based network pieces (i.e. software code and software architecture) for update and reengineering.
- Individual nations will define, categorize, and prioritize system components (corresponding to desired capabilities) for each nation's contributions

- Individual nations will define the means of communication between the components
- Individual nations will identify the core infrastructure needed to support the components.

During spiral 2,

- Jointly integrate policy-based networking software and demonstrate policy-based networking capability with all integrated components.
- Jointly demonstrate new capabilities on a frequent basis, if only to act as integration tests.
- Individual nations will ensure core (i.e. essential) and functional (i.e. used as building blocks) capabilities are implemented during this spiral, with some implementation of operational (i.e. exposed to other components) capabilities that demonstrate these new capabilities.

During spiral 3:

- Jointly participate in a full system demonstration using realistic scenarios showing how each nation's contribution meets the objectives and scope of this agreement.
- Jointly produce a joint technical paper for publication of the releasable, collaborative efforts over the project period.
- Individual nations will demonstrate their capabilities and concepts within different scenarios
- If resources permit, individual nations may add functionality by developing extension capabilities (i.e. optional, extra value capabilities), and demonstrate these with smaller, highly focused scenarios design to showcase the value added. The capabilities should approximate the full operational behavior and be capable of supporting the core demonstrations scenarios.

Meetings

In anticipation of the Project Arrangement getting signed through the respective embassies, a Face to Face meeting was planned and conducted in San Diego in October 2007. All nations took part and the US was represented by AFRL and SPAWAR. From a preplanned agenda many areas that would have to be explored for the PECC project were discussed. AFRL led the team members on a review and confirmation of the goal architecture, and began the development and expansion of a case scenario based upon a Combat Search And Rescue (CSAR) mission. Network traffic expected during different stages of the mission and the types of players that would be involved in the exchange of this traffic were identified. A view into the management architecture and at what points the management of network resources would take place were examined. Potential issues that would arise from implementing hierarchical versus independent management control were tabled until further research could be performed. The topic of dynamic group formation was briefly discussed and was defined in two ways. One scenario could be pursued in which a non-peer could be added into the network environment dynamically, say a visiting foreign dignitary, and the need to allow this person to leverage some services would be permitted. The second scenario that could be integrated into the larger case scenario would be to have groups of peers could enter

the network and form up connections dynamically, with different forces encountering each other and are able to “expose” services and share them with the group.

During the meeting, a breakout session took place in which different coalition members separated and privately discussed more specific areas of interest within the smaller group. The results of the discussions were summed up to the group as a whole. UK and US members explored the case scenario events, potential policy enabling of network resources, and overall network management aspects in general. The AUS, CAN and SPAWAR members explored the multi-bearer information sharing and the use of multi-topology routing aspects over various available classified and unclassified networks. A final discussion revolved briefly upon the test-bed connectivity and network layout which will be discussed in the next section.

RESULTS AND DISCUSSION

Architecture

The original architecture of CNMS follows closely the architecture of DoD certified solutions (e.g. Combined ENTerprise Regional Information eXchange system (CENTRIX)). After semi-annual meetings with PECC participants over the last 2 years, it was decided that PECC will follow the same logical architecture with minimal changes (see Figure 1), while updating the implementation to include IPv6 and a more modern service oriented architecture. The AFRL original CNMS architecture’s certification and accreditation (C&A) expired in September 2006. A new package was created in order to be ready for live experimentation.

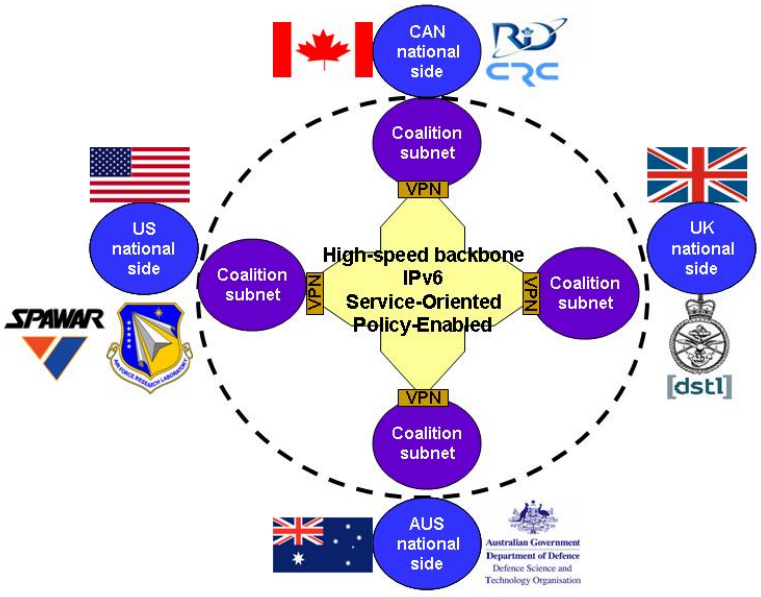

Figure 1 - PECC Basic Architecture

The new test bed to be used by PECC is called the Venture Assessment Network Guiding Users Actively Researching Dual-stacks (VANGUARD) and was created with the intention of exploring the next generation internet protocol called IPv6. Approval was given for IPv6 network management testing to be conducted on this test bed on a standalone basis, the results of which have been provided to the AF IPv6 Transition Office at the Air Force Communications Agency (AFCA), the DoD, and Congress. The results of the testing were useful not only in helping to successfully demonstrate IPv4/IPv6 equivalent performance in network management (one of the categories of the Joint Chiefs of Staff Operational Milestone Criteria) but also will provide useful data in network management implementation in the PECC scenario. The C&A package was submitted through AFRL Information Assurance (IA) office, AFRL HQ's IA office, and finally to the Designated Approval Authority (DAA) at AFMC HQ. Approval was finally received approximately eight months after initial submission. The accreditation is valid for three years which will follow the expected timeline for the PECC project.

Initial connectivity is being established at this present moment via IPSec tunnels. The PECC portion of the VANGUARD test bed will be dual stack running both IPv4 and IPv6 traffic. Additionally, the US has taken the lead in developing a new Service Oriented Architecture (SOA) based on eXtensible Markup Language (XML) using the eXtensible Messaging and Presence Protocol (XMPP) for use on the overall cross nation Wide Area Network (WAN). As part of the cross domain solution AFRL's ISSE guard has been set up on VANGUARD to prepare for sending SNMP traffic between high and low side domains.

Resource Management

The adopted PECC architecture will integrate mechanisms for resource management through the use of Semantically Augmented Resource Managers (SARM). The goal is to provide minimally intrusive resource management, using as few windows as possible. SARM will allow a network manager to focus on the tasks specific to each individual operator using one-glance awareness of task availability and caution panel style indicators. SARM will provide a reasoning agent that will have the ability to categorize network events and determine a common cause that produced the events or a potential problem that may result. Most network management and monitoring tools available commercially are "heavy weight" and require a thick client such as HP Openview or Smarts InCharge. Additionally a large footprint may be needed like using Oracle or Web Logic in order to do custom analysis for network managers. Lightweight network monitors with some rudimentary management capabilities are ideal for the network manager to reduce cost, time and labor. SARM makes use server-side components and client-side components and can be categorized as a lightweight tool. Its continued use in PECC will provide some excellent benefits to a policy enabled coalition environment.

CONCLUSIONS

The PECC PA should be signed by the beginning of 2008. Once the PA is signed, an official technical kick-off will happen with each nation's technical staff. The program leads of each of the nation's have agreed to begin initial architecture work (i.e. getting the labs connected), which is covered under disclosure agreements already in place under TP8.

Development continues on SARM and ISSE test bed integration, as well as refining the architecture based on updated national projects. Getting the GIG Network Centric Implementation Documents (NCIDs) released to the foreign nations involved in this work will help build more standardized methods of interaction between the test beds. With the approval of the use of VANGUARD, connectivity will happen shortly.

ACRONYMS

AFRL	Air Force Research Laboratory
CC3DE	Coalition Command Control & Comm Demo Environment
CIIMS	Coalition Information Infrastructure Management System
CNMS	Coalition Network Management System
DAA	Designated Approval Authority
IETF	Internet Engineering Task Force
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
JCS	Joint Chiefs of Staff
NM	network management
PA	Project Arrangement
PECC	Policy Enabled Coalition Communications
QoS	quality of service
RFC	Request for Comments
SARM	Semantically Augmented Resource Managers
SNMP	Simple Network Management Protocol
SOA	service oriented architecture
WAN	Wide Area Network
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol